

VOL. 1 · ISSUE 58

Cyber Shield

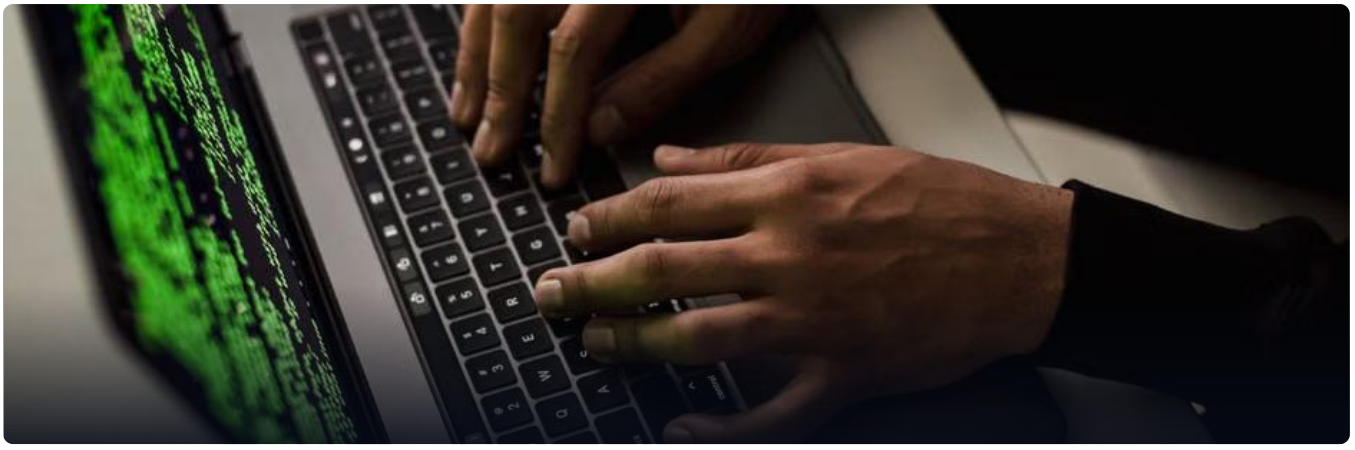
November 02, 2026

Essential cybersecurity intelligence for small and mid-sized businesses — powered by AI, delivered by Intelligent Automation, LLC.

INTELLIGENT AUTOMATION, LLC · INTELAMATION.COM · FAIRFIELD, NJ

FEATURE

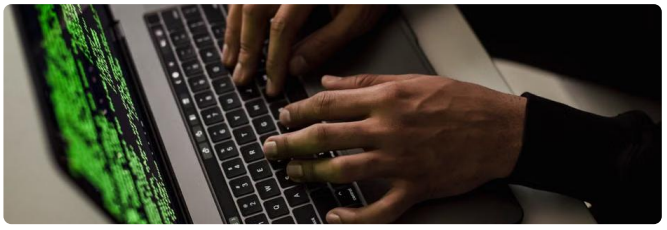
This Week in Cybersecurity



Critical Langflow Flaws Could Let Unauthenticated Attackers Run Code on Servers



Is Your SOC Ready for AI Agents? A Maturity Check Before You Deploy



Attackers Pose as IT Support on Microsoft Teams, Abuse AD CS to Steal Company Data

INTEL

Cyber Threat Intelligence



Critical Langflow Flaws Could Let Unauthenticated Attackers Run Code on Servers



Is Your SOC Ready for AI Agents? A Maturity Check Before You Deploy



Attackers Pose as IT Support on Microsoft Teams, Abuse AD CS to Steal Company Data

INTEL

Threat Intelligence — Continued

Government Linux Servers Targeted With SysGoRAT and Suspected AI-Generated Scripts

New VOLTA Infostealer Uses Claude, Gemini, and Kimi AI to Rank Victims by Financial Value

CVSS 10.0 LXD, MicroCloud Flaw Lets Attackers Impersonate Trusted Clients Without a Private Key

ISC Stormcast For Monday, November 2nd, 2026 https://isc.sans.edu/podcastdetail/10160, (Mon, Nov 2nd)

OneNote File Extraction, (Sun, Nov 1st)

💡 WEEKLY TECH TIP

Verify Before You Trust Internal Communication Requests

Attackers are impersonating IT support staff through internal platforms like Microsoft Teams to gain trust and steal credentials or data. These sophisticated social engineering attacks exploit employees' natural inclination to help colleagues and comply with IT requests.

Step 1: Establish a verification protocol for all unexpected IT support contacts or requests.

Step 2: Train employees to independently confirm requests through known phone numbers or in-person contact.

Step 3: Never share credentials, approve certificate requests, or install software from chat-only requests.

Step 4: Report suspicious internal messages to your security team immediately, even if uncertain.

ALERTS

National Cybersecurity Alerts

ISC Stormcast For Monday, November 2nd, 2026 https://isc.sans.edu/podcastdetail/10160, (Mon, Nov 2nd)

OneNote File Extraction, (Sun, Nov 1st)

Wireshark 5.0.0rc1 Release, (Sat, Oct 31st)

YARA-X 1.22.1 Release, (Sat, Oct 31st)

REGIONAL

Regional & Sector-Specific Alerts

ISC Stormcast For Monday, November 2nd, 2026 https://isc.sans.edu/podcastdetail/10160, (Mon, Nov 2nd)

OneNote File Extraction, (Sun, Nov 1st)

Wireshark 5.0.0rc1 Release, (Sat, Oct 31st)

🛡 NOVEMBER AWARENESS

Holiday Shopping Scams

Security Awareness Spotlight: Holiday Shopping Scams As your employees start their holiday shopping, cybercriminals are launching fake package delivery emails, bogus gift card offers, and fraudulent invoices that look identical to legitimate retailers. These scams don't just target personal accounts—many employees shop during work hours or use company emails for tracking, which means one wrong click can give hackers access to your business systems and customer data. The red flags to watch for include unexpected shipping notifications for orders you didn't place, urgent requests to "verify payment information," and deals that seem impossibly good, especially from sellers you've never heard of. **Action for today:** Send a quick message to your team reminding them that your company will never ask them to purchase gift cards to solve a problem, and they should forward any suspicious shipping or payment emails to you before clicking any links.

ACTION ITEM

Schedule a 15-minute team security review this week using this month's theme as your agenda.

SMB SPOTLIGHT

Protecting Your Business



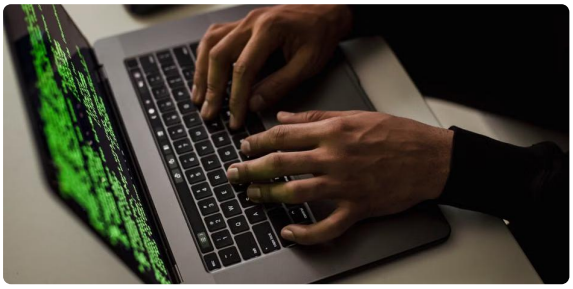
From industry concern to practical action: the value of working with regulators



Critical security issue affecting PHP



Introducing a new AI chapter in the NCSC research problem book



Using TLS to protect data

INNOVATION

Cybersecurity Advancements

Revolve Data Breach Impacts at Least 180,000 People

Google Introduces $250,000 Root-in-Cloud Bug Bounty Reward

Malicious Claude Code Extension Served in Cursor Supply Chain Attack

Chainalysis Discloses Data Breach Following AI-Driven Cyberattack

CTO'S DESK

From the Desk of Daniel Ramos



Daniel Ramos
Chief Technology Officer
Intelligent Automation, LLC | Fairfield, NJ
Managed Cybersecurity Service Provider

The convergence we've been warning about is here. This week's headlines tell a story that should concern every business leader: AI isn't just changing how we work—it's fundamentally transforming the threat landscape itself.

What strikes me most isn't any single vulnerability, but rather how attackers are weaponizing AI across the entire attack chain. They're using generative AI to craft more convincing social engineering attacks through Teams impersonation, deploying AI-generated scripts to evade detection on government servers, and even leveraging tools like Claude and Gemini to automatically prioritize which victims offer the richest financial rewards. Meanwhile, many organizations are racing to deploy AI agents in their security operations without proper maturity assessments.

Here's my takeaway: the asymmetry is real. Attackers are already using AI at scale, while most defenders are still figuring out their AI strategy. This gap will only widen if we don't act deliberately.

The good news? You don't need to become an AI expert overnight. Start by ensuring your fundamentals are solid—patch management, access controls, and security awareness training. Then thoughtfully explore how AI can strengthen your defenses. Let's close that gap together.

CONNECT WITH DANIEL
linkedin.com/in/iamdanielramos · daniel.ramos@intelamation.com



Your Cybersecurity Partner for the Digital Age

Serving small and mid-sized businesses since 2013

336 US Highway 46, Fairfield, NJ 07004

(888) 711-4521 · intelamation.com

Read online: newsletters.intelamation.net

© 2026 Intelligent Automation, LLC · All rights reserved